TITLE OF THE INVENTION

ENCRYPTION ALGORITHM MANAGEMENT SYSTEM

CROSS REFERENCE TO RELATED APPLICATION

This application claims benefit of priority to Japanese Patent Application No. 11-301842 filed October 25, 1999, the entire content of which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

This invention relates to an encryption algorithm management system that supervises encryption algorithms used in a data encryption system and may prevent the encryption algorithms from utilized carelessly and dishonestly.

DISCRIPTION OF THE BACKGROUND

Currently, the data encryption system, which utilizes encryption systems using the encryption algorithm and cipher-keys, is widely used in various computers that are connected to a network. In this kind of data encryption system, there are various encryption algorithms, which are used in different ways depending on the respective purposes.

Such encryption algorithms may be regulated to export in the United State etc. depending on how long and sophisticated the encryption algorithm is. However, these kinds of encryption algorithms are carelessly or dishonestly used by

unauthorized users due to development of an open network.

As described above, in the data encryption system, the encryption algorithm has been carelessly or dishonestly used due to the development of an open network.

SUMMARY OF THE INVENTION

Accordingly, one object of this invention is to provide an encryption algorithm management system that may prevent an encryption algorithm from utilized carelessly or dishonestly by supervising the encryption algorithm used for a data encryption system.

The present invention provides an encryption algorithm management system having a terminal unit and a center unit that have a common cipher-key to a ciphered encryption algorithm, the terminal unit includes a transmitter configured to transmit a demand to the center unit for obtaining an encrypted data needed for decrypting the ciphered encryption algorithm when the ciphered encryption algorithm is decrypted, and an encryption controller configured to renew the common cipher-key in case of receiving the encrypted data from the center unit in response to the demand, and to produce an encryption algorithm by decrypting the encrypted data with the renewed common cipher-key, the center unit includes a key controller configured to renew the common cipher-key so as to be identical with the renewed common cipher-key in case of receiving the demand from the transmitter and an encoder

configured to produce the encrypted data by encrypting a cipher-key with the renewed common cipher-key and to transmit the encrypted data to the terminal unit.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the invention and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

FIG. 1 is a block diagram showing an encryption algorithm management system of a first embodiment of the present invention;

FIG. 2 is a block diagram showing components of an encryption algorithm controller of the first embodiment;

FIG. 3 is a block diagram showing an encryption algorithm management system of a second embodiment of the present invention;

FIG. 4 is a block diagram showing components of an encryption algorithm controller of the second embodiment;

FIG. 5 is a block diagram showing an encryption algorithm management system of a third embodiment of the present invention; and

FIG. 6 is a block diagram showing components of a cipher-key information controller of the third embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Several embodiments of the present invention are hereinafter described referring to drawings.

In the embodiments, symbols "E(X)[Y]" or "E(Z,X)[Y]" represent encrypted data that a data "Y" is encrypted with a cipher-key "X" by using encryption algorithm "Z".

FIG. 1 is a block diagram showing an encryption algorithm management system of a first embodiment of the present invention. The encryption algorithm management system includes a center unit 10 and pluralities of terminal units 20i (i=1~n) connected to the center unit 10 via communication networks.

The center unit 10 includes a controller 11, a stream cipher such as a linear feedback shift resister 12, a cipher-key information memory 13 and an encoder 14.

The controller 11 verifies whether the terminal unit 20i is authorized to use an encryption algorithm on the basis of administrative information such as an expiration date or the like in case of receiving a demand from the terminal unit 20i. If the terminal unit 20i has the authorization, the controller 11 inputs a state value of "t", which is stored in a stream cipher 26 in the terminal unit 20i, into the stream cipher 12, and inputs an identification index "IDA1" into the cipher-key information memory 13.

The stream cipher 12 produces an output value "Kt" corresponding to the state value "t" from the controller 11 and inputs the output value "Kt" into the encoder 14.

The cipher-key information memory 13 memorizes cipher-keys "KAl" corresponding to the respective identification indexes IDAl and has a function of inputting the cipher-key "KAl" corresponding to the identification index IDAl outputted from the controller 11 into the encoder 14.

The encoder 14 has functions of encrypting the cipher-key "KAl" from the cipher-key information memory 13 by using the output value "Kt" of the stream cipher 12, and transmitting the encrypted data E1(Kt)[KAl], that is the encrypted cipher-key, to the terminal unit 20i.

The terminal unit 20i, which may be composed of a computer such as a personal computer, includes and controls a cipher-key information memory 21, an encryption algorithm memory 22, an encryption algorithm controller 23 and an encrypting and decrypting controller 24.

The cipher-key information memory 21 memorizes communication cipher-keys "Kij" needed for communicating with other terminal unit 20j (not shown). The terminal unit 20i controls the cipher-key information memory 21 to transmit the cipher-key "Kij" to the encrypting and decrypting controller 24.

The encryption algorithm memory 22 memorizes encrypted data E2(KAl)[Al], that is the ciphered encryption algorithm. The terminal unit 20i controls the encryption algorithm memory 22 to transmit the encrypted data E2(KAl)[Al] to the encryption algorithm controller 23.

The encryption algorithm controller 23 has functions of decrypting the encrypted data E1(Kt)[KAl] from the center unit 10 and then decrypting the encrypted data E2(KAl)[Al] from the encryption algorithm memory 22 on the basis of the decryption result of the encrypted data E1(Kt)[KAl], that is "KAI" or "ERROR". The encryption algorithm controller 23 finally inputs the decryption result of the encrypted data E2(KAl)[Al], that is "AI" or "ERROR", into the encrypting and decrypting controller 24.

As shown in FIG. 2, the encryption algorithm controller 23, which is stored in unreadable memory area that may not be rewritten by outsiders such as users, includes a controller 25, the stream cipher 26, a cipher-key decryption controller 27 and an encryption algorithm decryption controller 28.

The controller 25 has functions of inputting both the encrypted data E1(Kt)[KAl] into the cipher-key decryption controller 27 and the encrypted data E2(KAl)[Al] into the encryption algorithm decryption controller 28, and further inputting a creation signal "1" needed for creating the next state value into the stream cipher 26 in case of receiving both the encrypted data E1(Kt)[KAl] from the center unit 10 and the encrypted data E2(KAl)[Al] from the encryption algorithm memory 22.

The stream cipher 26 produces the output value "Kt" on the basis of the current state value "t" and memorizes a new state value "t+1" in case of receiving the creation signal

"1" from the controller 25. The stream cipher 26 then inputs the output value "Kt" into the cipher-key decryption controller 27.

The cipher-key decryption controller 27 decrypts the encrypted data E1(Kt)[KA1] by using the output value "Kt" as a common cipher-key, and inputs the decryption result of the encrypted data E1(Kt)[KA1], that is "KA1", into the encryption algorithm decryption controller 28.

The encryption algorithm decryption controller 28 decrypts the encrypted data E2(KA1)[A1] by using the decryption result "KA1" as a cipher-key, and inputs the decryption result of the encrypted data E2(KA1)[A1], that is an encryption algorithm "A1", into the encrypting and decrypting controller 24.

The encrypting and decrypting controller 24 encrypts a message "M", which is inputted by the terminal unit 20i itself, by using the encryption algorithm "A1" from the encryption algorithm decryption controller 28 and the communication cipher-key Kij from the cipher-key information memory 21, and transmits the encrypted data E(A1, Kij)[M] to the other terminal unit 20j.

An operation of the above-mentioned encryption algorithm management system is hereinafter described.

In the center unit 10, the controller 11 verifies whether the terminal unit 20i is authorized to use encryption algorithm on the basis of an expiration date or the like in case of receiving

a demand from the terminal unit 20i. If the terminal unit 20i has the authorization, the controller 11 inputs a state value of "t" of a stream cipher 26 in the terminal unit 20i into the stream cipher 12, and inputs an identification index of IDA1 into the cipher-key information memory 13.

The stream cipher 12 produces an output value "Kt" corresponding to the state value "t" from the controller 11 and inputs the output value "Kt" to the encoder 14.

The cipher-key information memory 13 inputs the cipher-key "KA1" corresponding to the identification index IDA1 outputted from the controller 11 into the encoder 14.

The encoder 14 encrypts the cipher-key "KA1" from the cipher-key information memory 13 by using the output value "Kt" of the stream cipher 12, and transmits the encrypted data E1(Kt)[KA1], that is the encrypted cipher-key, to the terminal unit 20i.

The terminal unit 20i controls the cipher-key information memory 21 to transmit the cipher-key "Kij" to the encrypting and decrypting controller 24 in response to the encrypted data E1(Kt)[KA1].

The terminal unit 20i controls the encryption algorithm memory 22 to transmit the encrypted data E2(KA1)[A1] to the encryption algorithm controller 23.

In the encryption algorithm controller 23, the controller 25 inputs both the encrypted data E1(Kt)[KA1] into the cipher-key decryption controller 27 and the encrypted data

E2(KA1)[A1] into the encryption algorithm decryption controller 28, and further inputs a creation signal "1" needed for creating the next state value into the stream cipher 26 in case of receiving both the encrypted data E1(Kt)[KA1] from the center unit 10 and the encrypted data E2(KA1)[A1] from the encryption algorithm memory 22.

The stream cipher 26 produces the output value "Kt" on the basis of the current state value "t" and memorizes a new state value "t+1" in case of receiving the creation signal "1" from the controller 25. The stream cipher 26 then inputs the output value "Kt" into the cipher-key decryption controller 27.

The cipher-key decryption controller 27 decrypts the encrypted data E1(Kt)[KA1] by using the output value "Kt" as a common cipher-key, and inputs the decryption result of the encrypted data E1(Kt)[KA1], that is "KA1", into the encryption algorithm decryption controller 28.

The encryption algorithm decryption controller 28 decrypts the encrypted data E2(KA1)[A1] by using the decryption result "KA1" as a cipher-key, and inputs the decryption result of the encrypted data E2(KA1)[A1], that is an encryption algorithm "A1", into the encrypting and decrypting controller 24.

The encrypting and decrypting controller 24 encrypts a message "M", which is inputted by the terminal unit 20i itself, by using the encryption algorithm "A1" from the encryption

algorithm decryption controller 28 and the communication cipher-key "Kij" from the cipher-key information memory 21, and transmits the encrypted data E(Al, Kij)[M] to the other terminal unit 20j.

According to the first embodiment, since a common cipher-key, that is the output value of the stream cipher, is renewed every time that the terminal unit 20i uses encryption algorithm "Al", the terminal unit 20i needs to obtain an encrypted data, which is encrypted with the common cipher-key, from the center unit 10. Accordingly, the encryption algorithm may be managed so as not to be utilized carelessly or dishonestly. Further, since the encryption algorithm controller 23 is stored in unreadable memory area that may not be rewritten by user, the encryption algorithm management system may prevent dishonest use of the encryption algorithm that is executed by means of backup of the memory area of the terminal unit 20i.

Furthermore, since the encryption algorithm controller 23 is stored in unreadable memory area that may not be rewritten by user, an unauthorized person may not tamper with the encryption algorithm controller 23.

Moreover, since the controller 11 verifies whether the terminal unit 20i is authorized to use encryption algorithm in case of receiving a demand from the terminal unit 20i and inputs a state value of "t" into the stream cipher 12 in order to obtain a common cipher-key "Kt" only if the terminal unit

20i has the authorization, the encryption algorithm may be managed on the basis of the authorization for the terminal unit 20i.

The effect of the tamper-resistance on the encryption algorithm controller 23 and the effect of the verification of authorization on the controller 11 may be achieved in the following embodiments in the same way as the first embodiment, although the operation and name of the encryption algorithm controller 23 change.

(Second embodiment)

FIG. 3 is a block diagram showing an encryption algorithm management system of a second embodiment of the present invention. FIG. 4 is a block diagram showing components of an encryption algorithm controller 30. A detail explanation of the same components as the components shown in FIGs. 1 and 2 are omitted by means of giving the same numerals as the components of the first embodiment to the same components. The only different components from the components shown in FIGs. 1 and 2 are mainly described herein.

The encryption algorithm management system of the second embodiment is a modified system of the first embodiment. In the second embodiment, a center unit transmits an encrypted data of encryption algorithm, that is ciphered encryption algorithm, instead of the encrypted data of the cipher-key. Further, a terminal unit transmits a demand to the center unit at every "n" times that the encryption algorithm is used, instead

of transmitting the demand every time.

Concretely speaking, the center unit 10a has an encryption algorithm memory 15 instead of the cipher-key information memory 13.

The terminal unit 20ia has a function of storing an encrypted data E2(Kt)[Al] including encryption algorithm "Al", which is transmitted from the center unit 10a, into the encryption algorithm memory 22. Further, as shown in FIG. 4, the terminal unit 20ia has the encryption algorithm controller 30 that includes a counter 32 instead of the encryption algorithm controller 23 shown in FIG. 2.

The encryption algorithm memory 15 memorizes encryption algorithm "Al" corresponding to the respective identification indexes IDAl and has a function of inputting the encryption algorithm "Al" corresponding to the identification index IDAl inputted by the controller 11 into the encoder 14.

The encoder 14 has functions of encrypting the encryption algorithm "Al" from the encryption algorithm memory 15 by using the output value "Kt" of the stream cipher 12, and transmitting the encrypted data E2(Kt)[Al], that is the ciphered encryption algorithm, to the terminal unit 20ia.

The encryption algorithm controller 30 has a function of counting the number of transmission of the encrypted data E2(Kt)[Al] from the encryption algorithm memory 22. Further, the encryption algorithm controller 30 has a function of inputting the encryption algorithm "Al", that is the decryption

result of the encrypted data E2(Kt)[Al], into the encrypting and decrypting controller 24 if the number of the transmission is less than "n" times, but inputting a random data, which is the decryption result in failure, into the encrypting and decrypting controller 24 if the number of the transmission is "n" times or over.

Concretely speaking, the encryption algorithm controller 30, which is stored in unreadable memory area that may not be rewritten by outsiders such as users, includes a controller 31, the counter 32, a stream cipher 33 and an encryption algorithm decryption controller 34.

The controller 31 has a function of inputting the encrypted data E2(KAl)[Al] into the encryption algorithm decryption controller 34 and a count signal "1" into the counter 32 in case of receiving the encrypted data E2(KAl)[Al] from the encryption algorithm memory 22.

The counter 32 memorizes the number of the count signals and has a function of increasing the number of the count signals by one in case of receiving the count signal "1" from the controller 31. Further, the counter 32 has functions of inputting a signal "0" into the stream cipher 33 if the renewed number of the count signals is less than an upper limit, which corresponds to the "n" times, of a permission to use the encryption algorithm, and inputting a signal "1" into the stream cipher 33 if the renewed number of the count signals is the upper limit or over.

The stream cipher 33 stores a new state value "t+1" and has functions of inputting the "Kt+1" corresponding to the state value "t+1" into the encryption algorithm decryption controller 34 in case of receiving the signal "1" from the counter 32, and inputting a value "Kt" that originates from the state value "t" into the encryption algorithm decryption controller 34 in case of receiving the signal "0" from the counter 32.

The encryption algorithm decryption controller 34 has a function of decrypting the encrypted data E2(Kt)[Al] by using the output value "Kt" from the stream cipher 33 as a cipher-key, and inputting the decryption result of the encrypted data E2(Kt)[Al], that is an encryption algorithm "Al", into the encrypting and decrypting controller 24. Further, the encryption algorithm decryption controller 34 has a function of inputting the decryption result in failure into the encrypting and decrypting controller 24 when the cipher-key is wrong.

An operation of the above-mentioned encryption algorithm management system is hereinafter described.

In the center unit 10a, the encryption algorithm memory 15 inputs the encryption algorithm "Al" corresponding to the identification index IDAl inputted by the controller 11 into the encoder 14 in case of receiving a demand from the terminal unit 20ia. The demand is transmitted every "n" times that encryption algorithm is used in the terminal unit 20ia.

The encoder 14 encrypts the encryption algorithm "Al" from the encryption algorithm memory 15 by using the output value "Kt" of the stream cipher 12, and transmits the encrypted data E2(Kt)[Al], that is the ciphered encryption algorithm, to the terminal unit 20ia.

The terminal unit 20ia stores the encrypted data E2(Kt)[Al] into the encryption algorithm memory 22, and controls the encryption algorithm memory 22 to transmit the encrypted data E2(Kt)[Al] to the encryption algorithm controller 30 every time that an encryption algorithm is used.

In the encryption algorithm controller 30, the controller 31 inputs the encrypted data E2(KAl)[Al] into the encryption algorithm decryption controller 34 and a count signal "1" into the counter 32 in case of receiving the encrypted data E2(KAl)[Al] from the encryption algorithm memory 22.

The counter 32 renews the number of the count signals so as to increase by one in case of receiving the count signal "1" from the controller 31. Further, the counter 32 inputs a signal "0" into the stream cipher 33 if the renewed number of the count signals is less than an upper limit, which corresponds to the "n" times, of a permission to use the encryption algorithm, and inputs a signal "1" into the stream cipher 33 if the renewed number of the count signals is the upper limit or over.

The stream cipher 33 inputs a value "Kt" correnponding to the current state value "t" into the encryption algorithm

decryption controller 34 in case of receiving the signal "0" from the counter 32, and inputting the value "Kt+1" that originates from the new state value "t+1" into the encryption algorithm decryption controller 34 in case of receiving the signal "1" from the counter 32.

The encryption algorithm decryption controller 34 decrypts the encrypted data E2(Kt)[Al] by using the output value "Kt" from the stream cipher 33 as a cipher-key, and inputs the decryption result of the encrypted data E2(Kt)[Al], that is an encryption algorithm "Al", into the encrypting and decrypting controller 24.

The encrypting and decrypting controller 24 encrypts a message "M", which is inputted by the terminal unit 20ia itself, by using the encryption algorithm "Al" from the encryption algorithm decryption controller 34 and the communication cipher-key "Kij" from the cipher-key information memory 21, and transmits the encrypted data E(Al, Kij)[M] to the other terminal unit 20j.

Further, the encryption algorithm decryption controller 34 inputs the decryption result in failure into the encrypting and decrypting controller 24 when the cipher-key is wrong.

In this case, the encryption algorithm decryption controller 34 outputs an error signal. As a result, a message "M" may not be encrypted with the encryption algorithm "Al".

As a matter of course, if the terminal unit 20ia correctly transmits a demand to the center unit 10a every "n" times that

an encryption algorithm is used, the correct encrypted data E2(Kt+1)[Al] can be obtained and stored into the encryption algorithm memory 22. In this case, the encryption algorithm decryption controller 34 correctly decrypts the encrypted data E2(Kt+1)[Al] by using the output value "Kt+1" from the stream cipher 33 as a cipher-key, and inputs the decryption result of the encrypted data E2(Kt+1)[Al], that is an encryption algorithm "Al", into the encrypting and decrypting controller 24.

As a result, the encrypting and decrypting controller 24 may correctly encrypt a message "M" by using the encryption algorithm "Al" and the communication cipher-key "Kij", and transmit the encrypted data E(Al, Kij)[M] to the other terminal unit 20j.

According to the second embodiment of the encryption algorithm management system, the encryption algorithm controller 30 counts the number of transmission of the encrypted data E2(Kt)[Al] from the encryption algorithm memory 22. Further, the encryption algorithm controller 30 inputs the encryption algorithm "Al", that is the decryption result of the encrypted data E2(Kt)[Al], into the encrypting and decrypting controller 24 if the number of the transmission is less than "n" times, but inputs a random data, which is the decryption result in failure, into the encrypting and decrypting controller 24 if the number of the transmission is "n" times or over.

Accordingly, since encryption algorithm may be used only if a cipher-key to the ciphered encryption algorithm, that is the state value, is correctly renewed in the center unit 10a, the encryption algorithm for the data encryption system may be managed, thereby preventing the encryption algorithm from utilized carelessly or dishonestly. Further, since the encryption algorithm controller 30 is stored in unreadable memory area that may not be rewritten by user, the encryption algorithm management system may prevent dishonest use of the encryption algorithm that is executed by means of backup of the memory area of the terminal unit 20ia.

(Third embodiment)

FIG. 5 is a block diagram showing an encryption algorithm management system of a third embodiment of the present invention. FIG. 6 is a block diagram showing components of a cipher-key information controller 40.

The encryption algorithm management system of the third embodiment is a modified system of the first embodiment. In the third embodiment, a terminal unit transmits a demand to the center unit every "n" times that a cipher key is used, instead of transmitting the demand every time.

The terminal unit 20ib has a function of storing an encrypted data E1(Kt)[KA1] including a cipher-key "KA1", which is transmitted from the center unit 10, into the cipher-key information memory 21b. Further, as shown in FIG. 6, the terminal unit 20ib has the cipher-key information controller

40 that includes a counter 43 instead of the encryption algorithm controller 23 shown in FIG. 2.

The cipher-key information memory 21b memorizes an encrypted data E1(Ki)[Kij] for a communication cipher-key "Kij" and stores the encrypted data E1(Kt)[KAl] transmitted from the center unit 10. The terminal unit 20ib may control the cipher-key information memory 21b to transmit both the encrypted data E1(Ki)[Kij] and the encrypted data E1(Kt)[KAl].

The cipher-key information controller 40 has a function of inputting the communication cipher-key "Kij", that is the decryption result of the encrypted data E1(Ki)[Kij], into the encrypting and decrypting controller 24 in case of receiving the encrypted data E1(Ki)[Kij] and the encrypted data E1(Kt)[KAl] from the cipher-key information memory 21b. Further, the cipher-key information controller 40 has a function of counting the number of transmission of the encrypted data E1(Kt)[KAl] from the cipher-key information memory 21b. Furthermore, the cipher-key information controller 40 has functions of inputting the cipher-key "KAl", that is the decryption result of the encrypted data E1(Kt)[KAl], into the encryption algorithm decryption controller 28b if the number of the transmission is less than "n" times, but inputting a random data, which is the decryption result in failure, into the encryption algorithm decryption controller 28b if the number of the transmission is "n" times or over.

The cipher-key information controller 40, which is stored

in unreadable memory area that may not be rewritten by outsiders such as users, includes a controller 41, a first cipher-key decryption controller 42, the counter 43, a stream cipher 44 and a second cipher-key decryption controller 45 as shown in FIG. 6.

The controller 41 has a function of inputting the encrypted data E1(Ki)[Kij], the encrypted data E1(Kt)[KAl] and a count signal "1" into the respective first cipher-key decryption controller 42, second cipher-key decryption controller 45 and counter 43 in case of receiving the encrypted data E1(Ki)[Kij] and the encrypted data E1(Kt)[KAl] from the cipher-key information memory 21b.

The first cipher-key decryption controller 42 has functions of decrypting the encrypted data E1(Ki)[Kij] by using a peculiar cipher-key "Ki" owned by the terminal unit 20ib, and inputting the decryption result of the encrypted data E1(Ki)[Kij], that is the communication cipher-key "Kij", into the encrypting and decrypting controller 24.

The counter 43 memorizes the number of the count signals and has a function of increasing the number of the count signals by one in case of receiving the count signal "1" from the controller 41. Further, the counter 43 has functions of inputting a signal "0" into the stream cipher 44 if the renewed number of the count signals is less than an upper limit, which corresponds to the "n" times, of a permission to use the encryption algorithm, and inputting a signal "1" into the stream

cipher 44 if the renewed number of the count signals is the upper limit or over.

The stream cipher 44 stores a new state value "t+1" and has functions of inputting the value "Kt+1" correnponding to the state value "t+1" into the second cipher-key decryption controller 45 in case of receiving the signal "1" from the counter 43, and inputting a value "Kt" that originates from the current state value "t" into the second cipher-key decryption controller 45 in case of receiving the signal "0" from the counter 43.

The second cipher-key decryption controller 45 has functions of decrypting the encrypted data E1(Kt)[KA1] by using the output value "Kt" from the stream cipher 44 as a cipher-key, and inputting the decryption result of the encrypted data E1(Kt)[KA1], that is the cipher-key "KA1", into the encryption algorithm decryption controller 28b. Further, the second cipher-key decryption controller 45 has functions of inputting the decryption result in failure into the encryption algorithm decryption controller 28b when the cipher-key is wrong.

The encryption algorithm decryption controller 28b has functions of decrypting the encrypted data E2(KA1)[A1] from the encryption algorithm memory 22 by using the decryption result "KA1" as a cipher-key, and inputting the decryption result of the encrypted data E2(KA1)[A1], that is an encryption algorithm "A1", into the encrypting and decrypting controller 24.

An operation of the above-mentioned encryption algorithm management system is hereinafter described.

The center unit 10 transmits the encrypted data E1(Kt)[KAl] including a cipher-key "KAl" to the terminal unit 20ib in case of receiving a demand for the encrypted data E1(Kt)[KAl] from the terminal unit 20ib.

The terminal unit 20ib stores the encrypted data E1(Kt)[KAl] into the cipher-key information memory 21b, and controls the cipher-key information memory 21b to transmit the encrypted data E1(Ki)[Kij] and the encrypted data E1(Kt)[KAl] to the cipher-key information controller 40 every time that an encryption algorithm is used.

In the cipher-key information controller 40, the controller 41 inputs the encrypted data E1(Ki)[Kij], the encrypted data E1(Kt)[KAl] and a count signal "1" into the respective first cipher-key decryption controller 42, second cipher-key decryption controller 45 and counter 43 in case of receiving the encrypted data E1(Ki)[Kij] and the encrypted data E1(Kt)[KAl] from the cipher-key information memory 21b.

The first cipher-key decryption controller 42 decrypts the encrypted data E1(Ki)[Kij] by using a peculiar cipher-key "Ki" owned by the terminal unit 20ib, and inputs the decryption result of the encrypted data E1(Ki)[Kij], that is the communication cipher-key "Kij", into the encrypting and decrypting controller 24.

The counter 43 memorizes the number of the count signals

and increases the number of the count signals by one in case of receiving the count signal "1" from the controller 41. Further, the counter 43 inputs a signal "0" into the stream cipher 44 if the renewed number of the count signals is less than an upper limit, which corresponds to the "n" times, of a permission to use the encryption algorithm, and inputs a signal "1" into the stream cipher 44 if the renewed number of the count signals is the upper limit or over.

The stream cipher 44 inputs the value "Kt" into the second cipher-key decryption controller 45 in case of receiving the signal "0" from the counter 43, and inputs a value "Kt+1" that originates from the new state value "t+1" into the second cipher-key decryption controller 45 in case of receiving the signal "1" from the counter 43.

The second cipher-key decryption controller 45 decrypts the encrypted data E1(Kt)[KA1] by using the output value "Kt" from the stream cipher 44 as a cipher-key, and inputs the decryption result of the encrypted data E1(Kt)[KA1], that is the cipher-key "KA1", into the encryption algorithm decryption controller 28b.

The encryption algorithm decryption controller 28b decrypts the encrypted data E2(KA1)[A1] from the encryption algorithm memory 22 by using the decryption result "KA1" as a cipher-key, and inputs the decryption result of the encrypted data E2(KA1)[A1], that is an encryption algorithm "A1", into the encrypting and decrypting controller 24.

The encrypting and decrypting controller 24 encrypts a message "M", which is inputted by the terminal unit 20ib itself, by using the encryption algorithm "Al" from the encryption algorithm decryption controller 28b and the communication cipher-key "Kij" from the first cipher-key decryption controller 42, and transmits the encrypted data E(Al, Kij)[M] to the other terminal unit 20j.

Further, the encryption algorithm decryption controller 28b inputs the decryption result in failure into the encrypting and decrypting controller 24 when the cipher-key is wrong.

In this case, the encryption algorithm decryption controller 28b outputs an error signal. As a result, a message "M" may not be encrypted with the encryption algorithm "Al".

As a matter of course, if the terminal unit 20ib correctly transmits a demand to the center unit 10 every "n" times that an encryption algorithm is used, the correct encrypted data E1(Kt+1)[KAl] can be obtained and stored into the cipher-key information memory 21b. In such case, the encryption algorithm decryption controller 28b correctly decrypts the encrypted data E1(Kt+1)[KAl] by using the state value "Kt+1" from the stream cipher 44 as a cipher-key, and inputs the decryption result of the encrypted data E1(Kt+1)[KAl], that is a cipher-key "KAl", into the encrypting and decrypting controller 24.

As a result, the encrypting and decrypting controller 24 may correctly encrypt a message "M" by using the encryption algorithm "Al" and the communication cipher-key "Kij", and

transmit the encrypted data E(Al, Kij)[M] to the other terminal unit 20j.

According to the third embodiment of the encryption algorithm management system, the cipher-key information controller 40 inputs the communication cipher-key "Kij", that is the decryption result of the encrypted data E1(Ki)[Kij], into the encrypting and decrypting controller 24 in case of receiving the encrypted data E1(Ki)[Kij] and the encrypted data E1(Kt)[KAl] from the cipher-key information memory 21b. Further, the cipher-key information controller 40 counts the number of transmission of the encrypted data E1(Kt)[KAl] from the cipher-key information memory 21b. Furthermore, the cipher-key information controller 40 inputs the cipher-key "KAl", that is the decryption result of the encrypted data E1(Kt)[KAl], into the encryption algorithm decryption controller 28b if the number of the transmission is less than "n" times, but inputs a random data, which is the decryption result in failure, into the encryption algorithm decryption controller 28b if the number of the transmission is "n" times or over.

Accordingly, since encryption algorithm may be used only if a cipher-key to the ciphered encryption algorithm, that is the state value, is correctly renewed in the center unit 10, the encryption algorithm for the data encryption system may be managed, thereby preventing the encryption algorithm from utilized carelessly or dishonestly. Further, since the

cipher-key information controller 40 is stored in an unreadable memory area that may not be rewritten by user, the encryption algorithm management system may prevent dishonest use of the encryption algorithm that is executed by means of backup of the memory area of the terminal unit 20ib.

In the first embodiment, although the terminal unit 20i transmits a demand for the encrypted data of a cipher-key to the center unit 10 every time an encryption algorithm is used in the terminal unit 20i, the terminal unit 20i may include a counter positioned between the controller 25 and the stream cipher 26 in the same way as the second and third embodiments. In such system, the terminal unit 20i may count the number of use of the cipher-key every time the encrypted data of the cipher-key is used, and may forbid using an encryption algorithm if the number of use of the cipher-key exceeds "n" times. That is, the terminal unit 20i may use the encryption algorithm only if the terminal unit 20i correctly demands the encrypted data of the cipher-key from the center unit 10 every "n" times.

Likewise, in the second and third embodiments, although the terminal units 10ia and 10ib count the number of use of the encrypted data transmitted from the center units 10a and 10 by means of the counters 32 and 43, and forbid using an encryption algorithm if the number of use of the encrypted data exceeds "n" times, the terminal units 10ia and 10ib may dispense with the counters 32 and 43, and may demand the encrypted data from the center unit 10 every time the encrypted

data is used in the same way as the first embodiment. According to such system, the similar effect may be achieved.

In every embodiment, although each of the stream ciphers 12 of the center units 10 and 10a receives a state value "t" and then outputs the value "Kt" correnponding to the state value "t", the stream cipher 12 may be substituted to a key generator that may produce the output value "Kt" on the basis of the state value "t" in a predetermined procedure, for example, a random number generator that may generate a random number in a predetermined sequence. Likewise, the key generator may be substituted for the stream ciphers 26, 33 and 44 of the terminal units 10i, 10ia and 10ib. According to the above-mentioned system, the similar effect may be achieved.

The operation of the encryption algorithm management system described in every embodiment may be stored in a medium as a program that can be executed by computer so as to be delivered easily. The medium is, for example, a magnetic disc, a floppy disc, a hard disc, a laser disc such as CD-ROM , CD-R, DVD or the like, a laser magnetic disc such as MO or the like, a semiconductor memory or the like. The medium is not limited to the above-mentioned examples provided that the medium is a computer-readable medium that may store a computer program.

An OS (Operating System) that operates on the basis of instructions of a program installed from the medium, or an MW (Middle-ware) such as a database managing software, a network software or the like, may execute a part of the operation of

the encryption algorithm management system described in every embodiment.

Further, the medium is not limited to a separated medium from computer. That is, the medium also means a medium that downloads or temporarily downloads a program transmitted through a LAN, the Internet or the like.

Furthermore, the medium is not limited to a single medium. That is, the medium may consist of a plurality of medium that executes the entire operation of the encryption algorithm management system.

The computer may consist of a single computer such as a personal computer or the like, or a computer system having a plurality of computer connected to each other through a network.

Further, the computer is not limited to a personal computer. The computer means a device or an apparatus, for example a processor of an information processing system or a microprocessor, which are capable of operating functions of the encryption algorithm management system by means of computer program.

According to the present invention, it is realized to provide an encryption algorithm management system that may prevent encryption algorithm from utilized carelessly or dishonestly by supervising the encryption algorithm used for a data encryption system.

Various modifications and variations are possible in light

of the above teachings. Therefore, it is to be understood that within the scope of the appended claims, the present invention may be practiced otherwise than as specifically described herein.